AMENDMENT TO THE CLAIMS

1.-28. (Canceled)

29. (Previously Presented) A security system for securing access to an operating system of a computer having at least a host central processing unit (CPU), computer memory means used by the host CPU to load programs from the operating system in order to operate the computer, ~~and~~ a storage device for storing data to be used by the computer; and a chain of components connecting the CPU to the storage device, the security system comprising:

a security partition formed in the storage device, the operating system being stored in the security partition; and

blocking means for intercepting communications and selectively blocking data access between the host CPU and the security partition, wherein the blocking means are deployed along the chain of components that connect the CPU to the storage device.

30. (Previously Presented) The security system as claimed in claim 29, wherein each user of the computer has an associated access profile, each access profile comprising information indicative of the level of access to portions of the storage device permitted by a user, and the blocking means controlling access to the storage device by a user in accordance with the access profile associated with the user.

31. (Previously Presented) The security system as claimed in claim 30, wherein the security system is arranged such that at least two different data access profiles are defined, one access profile ascribing read and write access to said security partition, and the other access profile not ascribing write access to said security partition.

32. (Previously Presented) The security system as claimed in claim 29, wherein said blocking means is independent and separately configurable of said host CPU.

33. (Previously Presented) The security system as claimed in claim 29, wherein during operation of the operating system the security system is arranged to divert and write operating system files to a location different to the security partition so that normal operation of the operating system continues even though operating system files in the secure partition have not been updated.

34. (Previously Presented) The security system as claimed in claim 33, wherein the security system is arranged to divert and write operating system files to a flash ROM.

35. (Previously Presented) The security system as claimed in claim 33, wherein the security system is arranged to divert and write operating system files to an invisible partition formed in the storage device.

36. (Previously Presented) The security system as claimed in claim 30, further comprising authentication means for authenticating a user of the computer and associating the user with a prescribed access profile, said blocking means controlling subsequent access to the security partition in accordance with the access profile associated with the user.

37. (Previously Presented) The security system as claimed in claim 29, wherein said blocking means includes processing means for controlling operation of said blocking means.

38. (Previously Presented) The security system as claimed in claim 30, wherein said blocking means is configured to block all access by the host CPU to the storage device before

initialisation of the security system, and to selectively permit access immediately after said initialisation in accordance with a respective access profile.

39. (Previously Presented) The security system as claimed in claim 38, wherein said authentication means enables a software boot of the computer to be effected only after correct authentication of a user, and said security system permits normal loading of the operating system during the start up sequence of the computer following said software boot.

40. (Currently Amended) The security system as claimed in claim 29, wherein said blocking means is a security device physically ~~disposed in line with the~~ deployed between an interface adapter and the storage device within a data access channel of the chain of components connecting ~~between~~ the host CPU and the storage device.

41. (Currently Amended) The security system as claimed in claim 39, wherein said blocking means is ~~disposed as part of~~ deployed as logic implemented by a bridging circuit within the chain of components connecting the host CPU and the storage device or within the storage device.

42. (Currently Amended) A method for securing access to an operating system of a computer, the computer having at least a host central processing unit (CPU), a storage device for storing data to be used by the computer, a chain of components connecting the host CPU to the storage device, and memory used by the host CPU to load programs from the operating system in order to operate the computer and storage device, the method comprising:

forming a security partition in the storage device;

storing the operating system in the security partition; and

at a first component deployed along the chain of components connecting the host CPU to the storage device, intercepting communications and selectively blocking data access between the host CPU and the security partition.

43. (Previously Presented) The method as claimed in claim 42, further comprising associating each user with an access profile comprising information indicative of the level of access to portions of the storage device permitted by a user; and

for each user, selectively blocking access between the host CPU and the security partition in accordance with the access profile defined for the user.

44. (Previously Presented) The method as claimed in claim 43, further comprising defining at least two different access profiles, one access profile ascribing read and write access to data stored on said security partition, and the other access profile not ascribing write access to said security partition.

45. (Previously Presented) The method as claimed in claim 43, further comprising authenticating a user of the computer, and associating the user with an access profile after successful user authentication.

46. (Previously Presented) The method as claimed in claim 42, wherein said selective blocking comprises controlling access between the host CPU and the security partition independently of the host CPU.

47. (Previously Presented) The method as claimed in claim 42, wherein said selective blocking comprises totally blocking access to the storage device by the host CPU during

initialisation of the computer, and intercepting all said access immediately after said initialisation and before loading of the operating system of the computer.

48. (Previously Presented) The method as claimed in claim 45, including performing a software boot of the computer only after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer after said software boot.

49. (Previously Presented) The method as claimed in claim 42, further comprising diverting and writing operating system files to a location different to the security partition during operation of the operating system so that normal operation of the operating system continues even though operating system files in the secure partition have not been updated.

50. (Previously Presented) The method as claimed in claim 49, wherein the operating system files are diverted and written to a flash ROM.

51. (Previously Presented) The method as claimed in claim 49, wherein the operating system files are diverted and written to an invisible partition formed in the storage device.

52. (Previously Presented) The method as claimed in claim 42, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

53. (New) The method as claimed in claim 42, wherein the first component is a dedicated hardware device comprising a dedicated CPU for processing the intercepted communications

and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition.

54. (New) The method as claimed in claim 42, wherein the first component is a bridging circuit comprising logic for processing the intercepted communications and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition.